UCSD Cybersecurity Bootcamp

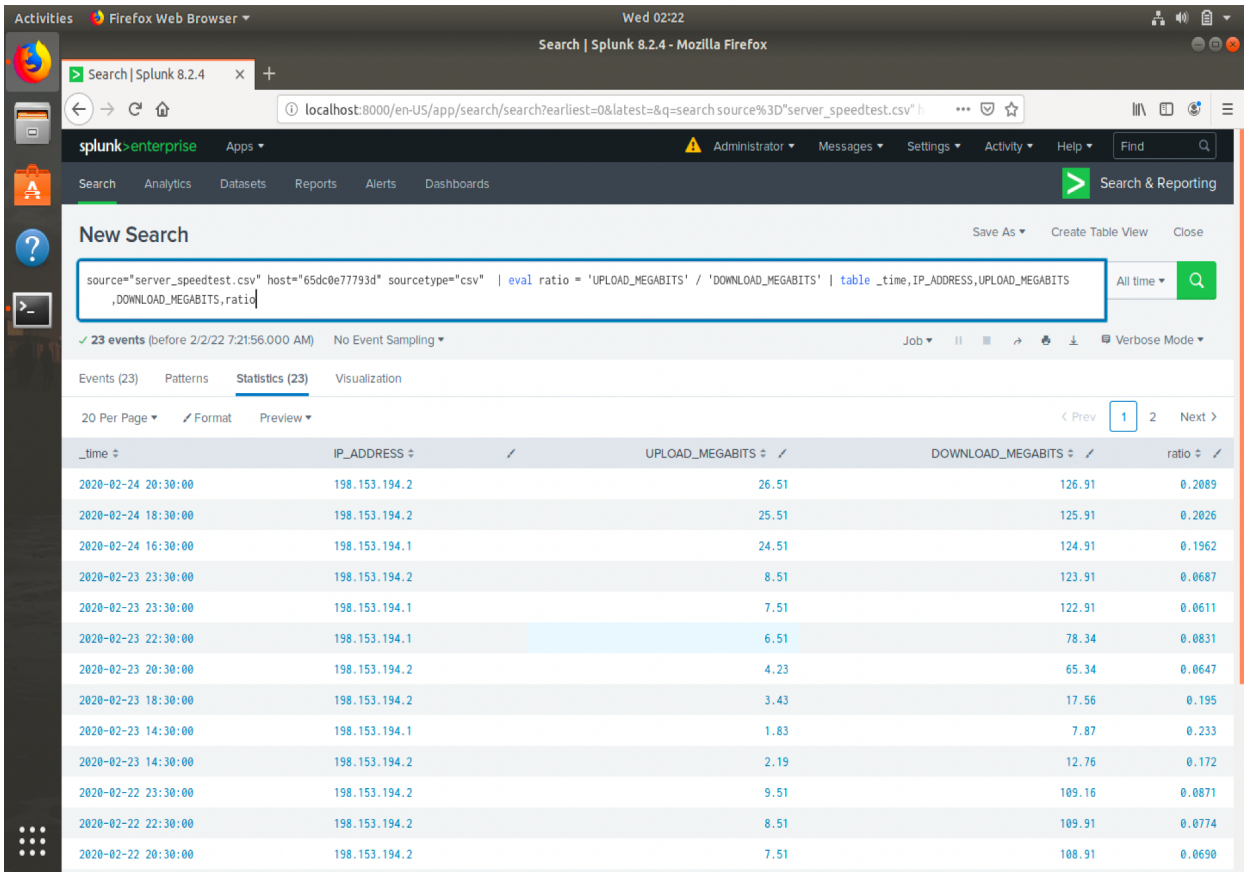
SIEMS Week 1 Homework

Introduction

This assignment is to demonstrate the core concepts of the Splunk software.

Step #1 : The Need For Speed

We are tasked with creating a search field in which we can see the effect a recent DDos attack has had on the upload and download speeds at the Vandalay corporation. Additionally we are requested to make a table in the report to show findings.

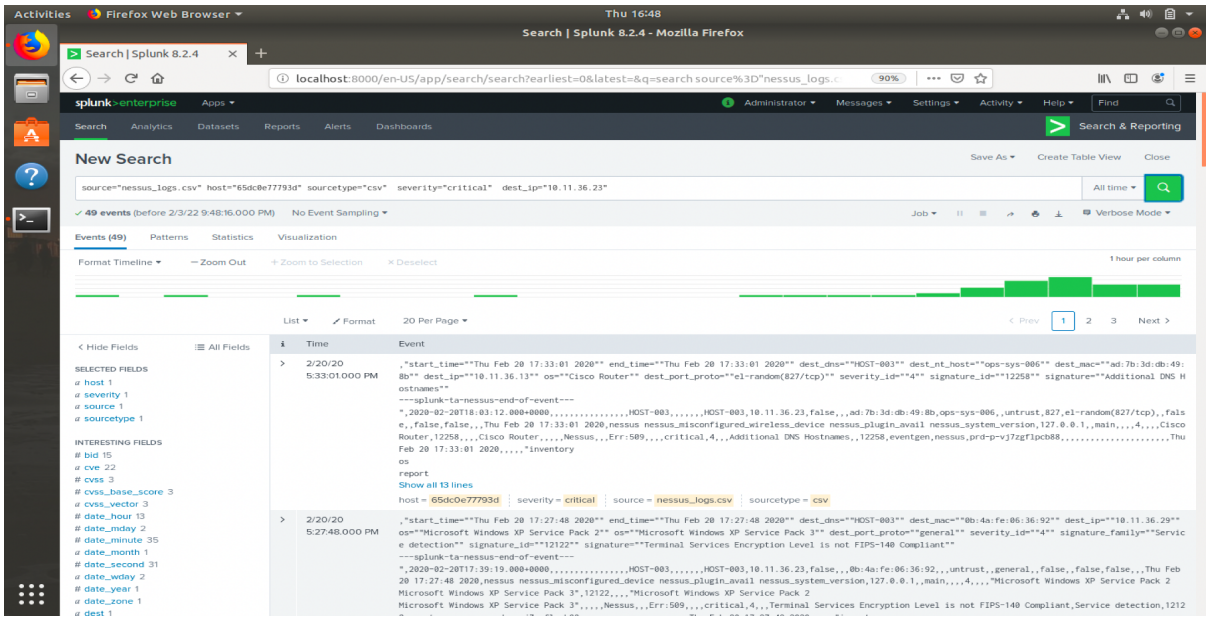


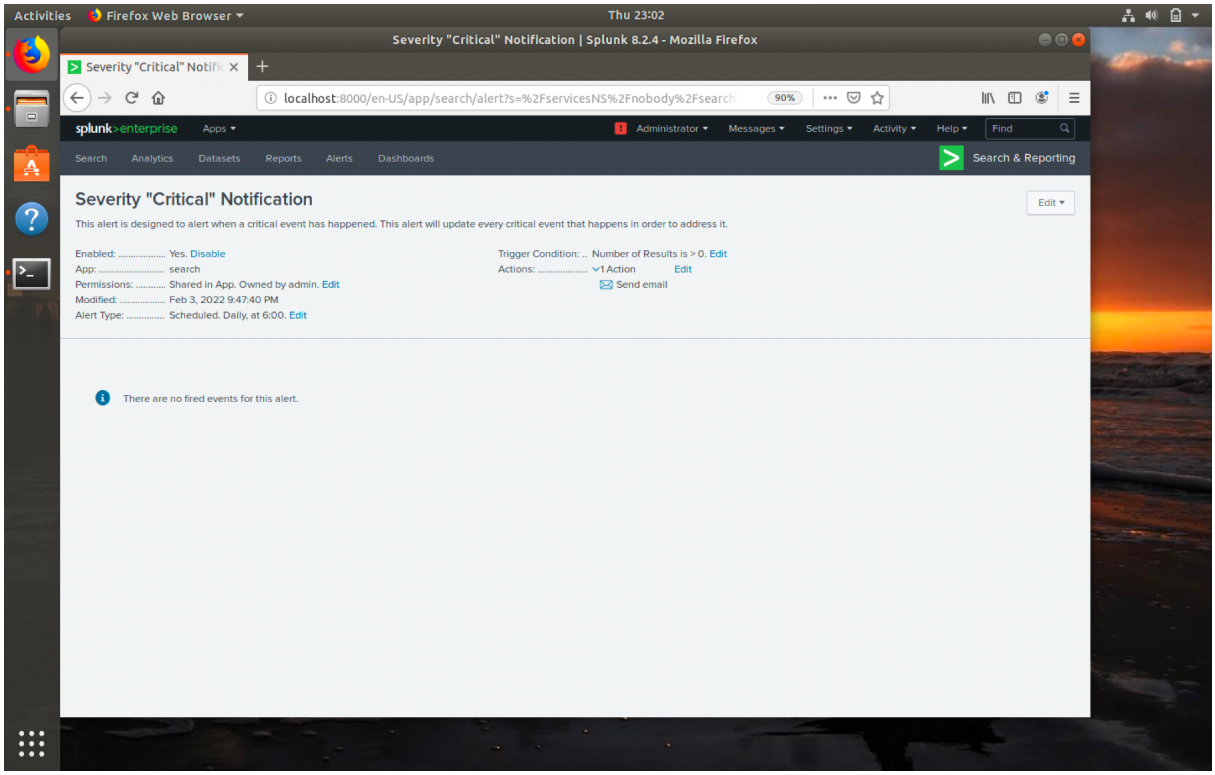
1.Based on the report, the attack happened on 2-23-2020 at 14:30.

2. The systems took approximately 9 hours to recover to baseline.

Step #2 : Are We Vulnerable

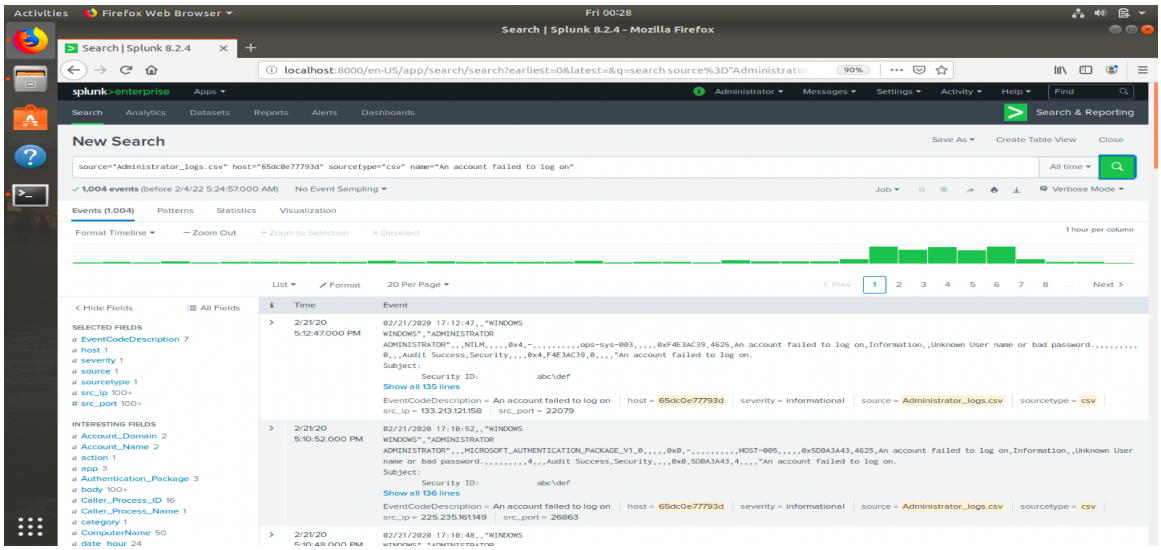
We are tasked with finding the critical vulnerabilities on the database then creating an alert to monitor for future critical events. This is shown in the screenshots below.





Step #3: Drawing the (base)line

We are tasked with monitoring the Admin logs for failed login attempts. We are then required to figure out what a baseline is for the Admin and create an alert to trigger when that threshold has been exceeded.



Based on the report shown the attack began at 0800 on 2/21/2020 and continued until 1400. The entire attack was 6 hours until the baseline returned.

The baseline for the failed logins was estimated at 20 attempts an hour with 30 being the threshold set for the alert.

The alert created can be viewed below: